

Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Please amend the claims as follows

- 1 1. (Original) A packet interception system for intercepting message packets transferred over a
2 network, the packet interception system comprising:
 - 3 A. a processed packet store; and
 - 4 B. an intercepted packet processor configured to process a currently intercepted message
5 packet and a hash value generated for a previously-processed message packet in
6 connection with a selected hash algorithm to generate a hash value for the currently-
7 intercepted message packet thereby to generate a processed message packet and to store
8 the processed message packet in the processed packet store.
- 1 2. (Original) A packet interception system as defined in claim 1 in which one of said currently-
2 intercepted message packet is a first intercepted message packet, the intercepted packet processor
3 being configured to use a selected value along with the first intercepted message packet in
4 generating the processed message packet therefore.
- 1 3. (Original) A packet interception system as defined in claim 2 in which the selected value
2 includes a session identifier value.
- 1 4. (Original) A packet interception system as defined in claim 1 in which said intercepted
2 packet processor is further configured to append to each currently-intercepted message packet a

3 time stamp reflective of a time at which the currently-intercepted message packet is received, the
4 time stamp further being used in generating the hash value.

1 5. (Original) A packet interception system as defined in claim 1 in which said intercepted
2 packet processor is further configured to generate, for selected processed message packets,
3 respective digital signatures, and to store each digital signature in the processed packet store with
4 the respective processed message packet for which it was generated.

1 6. (Original) A packet interception system as defined in claim 1 further including an intercept
2 system monitor configured to monitor at least one predetermined aspect of operation of said
3 packet processor, the intercept system monitor communicating with said packet processor over a
4 wireless communication link.

1 7. (Original) A method of processing message packets intercepted over a network, the method
2 comprising the steps of:

3 A. an intercepted packet processing step in which a currently-intercepted message packet is
4 processed in connection with a hash value generated for a previously-processed message
5 packet using a selected hash algorithm to generate a hash value for the currently-
6 intercepted message packet thereby to generate a processed message packet

7 B. storing the processed message packet in a processed packet store.

1 8. (Original) A method as defined in claim 7 in which one of said currently-intercepted message
2 packet is a first intercepted message packet, the intercepted packet processing step including a
3 step of using a selected value along with the first intercepted message packet in generating the
4 processed message packet therefore.

1 9. (Original) A method as defined in claim 8 in which the selected value includes a session
2 identifier value.

1 10. (Original) A method as defined in claim 7 in which said intercepted packet processing step
2 includes the step of appending to each currently-intercepted message packet a time stamp
3 reflective of a time at which the currently-intercepted message packet is received, the time stamp
4 further being used in generating the hash value.

1 11. (Original) A method as defined in Claim 7 in which said intercepted packet processing step
2 includes the step of generating, for selected processed message packets, respective digital
3 signatures for storage in the processed packet store with the respective processed message packet
4 for which it was generated.

1 12-23. (Cancelled)

Claim 1 specifically provides for the "process[ing of] a currently intercepted message packet and a hash value generated for a previously-processed message packet in connection with a selected hash algorithm to generate a hash value for the currently-intercepted message packet . . ." (emphasis added). Claim 7 has a similar limitation, in which the hash value of a previous packet is used to calculate the hash value for the current packet.

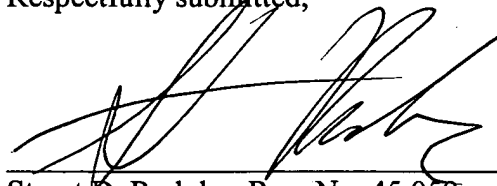
Thus, Applicant believes independent claims 1 and 7 are allowable as currently presented.

Claims 2 through 6 and 8 through 11 are dependent on claims 1 and 7, respectively, and are allowable for the same reasons as set forth above.

For the foregoing reasons, the claims as they now stand are patentable over the art of record, and withdrawal of the rejections and allowance of the pending claims is earnestly solicited. Should the Examiner believe that direct contact with the Applicant's attorney would advance the prosecution of this application, the Examiner is invited to telephone the undersigned at the number listed below.

An early Notice of Allowance is earnestly solicited.

Respectfully submitted,



Stuart D. Rudoler, Reg. No. 45,059
Wolf, Block, Schorr and Solis Cohen LLP
1650 Arch Street, 22nd Floor
Philadelphia, PA 19103
215-977-2484 (Phone)
215-405-3984 (Fax)